Inaugural lecture prof.dr. Sandro Etalle

Nice to know

Presented on 3 October 2008
at the Eindhoven University of Technology

Introduction

This lecture is in English not only because I think that English is by now the natural language for research in computer science, but also because my family, my sister and some of my international PhD students are here. I want to thank them for this and I think they have the good right to understand what I'll be saying.

I'll also try to make this lecture comprehensible by a non-technical public, at the cost of some scientific imprecision. So I'll call a cryptographic key a password, and commit a couple of other heresies.

A lesson we have not learned

I want to start from the old example of the 'man-in-the-middle' attack. I know some of the researchers here will immediately think this is terribly old-fashioned, but there are a couple of very up-to-date lessons we can learn from it.

What is a 'man-in-the-middle' attack? The most illustrative example of it is the famous 'MIG in the middle' [1] reported by Ross Anderson in his book. As Anderson himself admits, this is perhaps not historically accurate, but its principles are certainly valid, and it is now part of the security folklore.

The story has it that there were two parties at war with each other in Africa: on the one hand South Africa and Namibia, and on the other hand Angola supported by Cuba. Both parties had air forces and radar. Now, one of the concerns you have when you use both radar and airplanes is to have an accurate system to distinguish friend from foe: when you see an airplane trace on your radar, you want to know whether you should shoot at it or let it pass. For this purpose, the South African Air Force had allegedly adopted a rather nifty scheme based on cryptography, which worked more or less as follows:

The air base and the airplanes all shared a secret password (a cryptographic key, actually) *p* that could be used to encipher and decipher messages. Every time the radar detected an airplane in its range it would send a message consisting of a randomly generated secret code, enciphered using the secret password, asking the airplane to decipher the message. Since only friendly airplanes were in possession of the secret password, they were the only ones able to decipher the original message. So if the airplane detected by the radar was able to decipher the message, everyone at the air base would assume it to be a friendly one, and let it pass.

As it happens, this assumption was based on wrong premises, and here is what apparently happened at that point in history.

The enemy (that is, the Angolans, with the support of Cuba) stationed a few MIGs just outside the Namibian border. These MIGs sat and waited until a flight of South African bombers crossed the border to raid a target in Angola. When this happened, they took off, but rather than going after the South African airplanes, they entered the Namibian airspace to hit a South African camp in Northern Namibia. The South African radars detected the MIGs, but let them pass.

So how did the MIGs manage to get through the South African defenses? By pretending they were friends and not enemies, and they managed to convince the SAAF of this as follows. As soon as the SAAF radar detected them, it challenged them with a new random message enciphered with the secret password.
The MIGs could not decipher the message themselves, but what they did was to immediately relay this message to their *own* radar, which in turn sent it to the South African airplanes which were at that moment in Angolan airspace. The South African airplanes didn't know any better than that they had to decipher the message.
Which is just what they were programmed to do every time they received such a communication. So that's what they did, and they sent the deciphered messages back to the Angolan radar, which in turn sent them to the MIGs, which in turn sent them to the South African radar, which then assumed that the MIGs were actually friendly planes. And therefore allowed them to pass. This whole relay chain may have taken place in just a few hundredths of a second, so there was actually no way for the South African radar to know any better.

So, this is a 'man-in-the-middle' attack: someone convincing you of being someone else by relaying some of the message and the questions you send him to the one he pretends to be. Indeed, the MIGs would have never been able to defeat the South African radar without the help of the South African airplanes!
This is a very, very old kind of security problem: the history of failures of security protocols is indeed a surprisingly long one. Security protocols have been around for thirty years now, and people have started finding literally hundreds of crucial bugs in them starting already in 1995, when Gavin Lowe analyzed the security of a well-known security protocol (Needham-Schroeder's Protocol) by using a model checker. He did not manage to prove the protocol right, but instead he found a fundamental failure in it, which in that case could be easily fixed. The protocol was a very well known three-liner, and one of the interesting parts of the story is that this flaw had remained unnoticed under everyone's eyes for almost twenty years.
A new research area was born: the application of formal methods to security.
In the subsequent years researchers all over the world had fun cracking all sorts of security protocols, and only a few of them survived the battlefield.

figure 1

Needham-Schroeder's Protocol

$$\begin{aligned} &A \rightarrow B\text{: } \{Na,A\}_{PK(B)} \\ &B \rightarrow A\text{: } \{Na,Nb\}_{PK(A)} \\ &A \rightarrow B\text{: } \{Nb\}_{PK(B)} \end{aligned}$$

By 2003, we had enough knowledge and tools to honestly say that we knew how to design and debug security protocols. So from that point on things should have gone better. But they did not, and – among various failures found after that – I would like to mention a bug in the public-key version of the widely-used Kerberos algorithm found by Cervesato *et al*. in 2005, and – *dulcis in fundo* – an incredible bug in a single sign-on system used worldwide that was found just a few months ago by Luca Viganò, Luca Compagna and Alessandro Armando and the team of the Avantassar project (I am not allowed to give details at the time of writing). The bug is very similar to the one found in 1995 in the Needham-Schroeder protocol, in that it truly allows someone to impersonate someone else (also in the practical implementation), and it should not have been around in 2008.
So the first lesson we learn from this is not quite about research but about education. When you look at security, Murphy's law is a rule:

> Unless you can prove your protocol works correctly, it is not going to work.

And if you can prove your protocol works correctly, you are not even halfway through the process of building a secure system. I hope the Dutch government will take this into consideration when addressing high-impact issues such as *rekeningrijden* (or road pricing).

Accepting reality

So, security protocols can have design flaws, which is a problem. But this does not mean that if we ever managed to fix all the flaws of all the security protocols out there, we would be safer once and for all. This is not so, because security is always based on a chain of elements linked to each other, and somewhere along the chain there is usually a weak link. Take for instance something we all use: internet banking. Banks in the Netherlands offer excellent internet banking services, which are much more secure and advanced than those offered in other countries (like Italy, for instance). Really state-of-the-art stuff. Still, they are vulnerable to a reasonably simple yet surprisingly effective 'man-in-the-middle' attack. In this case, this is commonly called a 'man-in-the-*browser*' attack. So let's see in a minute how internet banking works with an example.

1. First, once I am logged-in, I type in the computer my order, say "please transfer 5000 euro to bank account number 12345 belonging to John Smith".
2. Then the computer tells the bank "Sandro wants to transfer 5000 euro to bank account number 12345 belonging to John Smith".
3. At that point the bank wants to make sure that it really is me who gave the order. So it sends a secret message, enciphered with a secret password, to my computer. That is the number I see on the screen.
4. I put my card in the bank's reader, I type in my PIN code, and then the number I see on the screen. Then I read on the screen of the reader the response to the first message, and I type the response in the computer.
5. The computer then sends this response to the bank, which checks if this is correct. The first message (the 'challenge') can only be correctly deciphered by someone who has a reader together with (a) my bank card and (b) my PIN code. So if the answer is correct, the bank can safely assume that the order actually came from me, and not from someone else trying to impersonate me.

So then the bank is sure that the order comes from me. But what can go wrong here is that my *browser* (Internet Explorer, Firefox etc.) at step (2) modifies the order slightly as follows: "Sandro wants to transfer 100 euro to bank account number 12345 belonging to John Smith *and 4900 euro to bank account number 54321 belonging to Mr. X*". The rest of the protocol remains unmodified, and

I have no way of checking that the order being carried out is not the one I intended. Of course, a browser does not usually modify bank orders, unless it has been maliciously hacked by someone, for instance by a virus or Trojan horse. But hacking a browser is not that difficult, and if the hacking has been done well, then when I ask it to show all transactions I have done in a certain period, it will hide the payment to Mr. X and show the original amount on the payment to John Smith. We have had a student develop such a hack, and the code he needed to write was less than a thousand lines of code long.

Should we stop using internet banking? No. We don't stop driving cars simply because it is dangerous, do we?

Should we worry? Yes. Just like we worry about the possibility that people may break into our house.

Can we do something about this? Certainly yes. To start with we can use one computer to visit untrusted sites and download untrusted software from the internet, and *another* computer to do business and internet banking. Again, the challenge here is education and awareness, and I think the Netherlands is doing a good job at that.

And then the crucial question:
Can we make 100% sure that we will not be the victim of such an attack? No. It can happen to everyone, me included. The fundamental reason for this is that our operating systems (XP, Vista, Linux, MacOS) and the programs we use everyday are too complex to be trustworthy, and no matter how much effort the software houses put into securing them, they will always contain tens of thousands of vulnerabilities which can be exploited by hackers to do all sorts of things, like hacking the browser as we just saw, or installing a keylogger which will make a note of my password and my credit card number and mail them back home to the hacker.
So the sad truth is that 100% security is unachievable.

Capitalizing

So far we've had a tiny little taste of the past and the present of security. What about the future?

Computer security presents a number of formidable challenges that will keep researchers' lives interesting for years to come. What my *personal* challenge is about is achieving *reasonable insecurity*.

To explain this, let me take a step back and give a simple example. Every day in our work we deal with electronic documents which should not be disclosed to just anyone: like my electronic health record, a new marketing strategy, a new idea for an industrial product. On the one hand, to be useful, this data needs to circulate around the organization we work in, like the company, the hospital etc. On the other hand, to guarantee its security we require some kind of *policy enforcement:* we want to make sure that the data is used and distributed according to some policies we have agreed upon. This policy states who may see and/or modify the document. It could say for instance that a certain letter may be seen only by senior management. Computer systems help us to guarantee policy enforcement in all sorts of ways, ranging from access control to document management systems. These systems are also there to guarantee that confidential data does not end up in the wrong hands. However, they work only *as long as we remain within our domain*: our office, our institute, our hospital. So within a single company, things go well. But what happens when my company cooperates with another company? (Let's say it outsources part of the work.) In that case, I have to send my documents to a different domain, and what can our computer systems do to guarantee policy enforcement in this new setting?

Nothing at all. Once a document has left my domain, I have lost *all* control of it. I may wish that my letter be read only by senior managers, but I have no guarantee that this policy will be followed.

So what do we do in this situation? We place our hopes on lawyers and auditors, and write immensely complex *non-disclosure agreements*, which promise the most awful consequences should the documents we share not be treated confidentially. This solution is of course not satisfactory; it only shows our inability to deal with the problem. I think that – when it comes to policy enforcement – we are still in the middle ages of security.

The fundamental reason why access control systems are of no help across organizations is that they work in a *preventive* manner: they are designed to *block* all actions that are not explicitly authorized before they take place. This makes them extremely powerful, but also inflexible. Moreover, we have just seen that 100% security does not exist anyhow, so why don't we look at solutions that guarantee less security but also work across domains?

Having preventive policy enforcement systems in our 'liquid society' is also quite unreasonable: Imagine the world as it would be if law enforcement was primarily done by preventive means. Some 'infrastructure' would have to stop us from doing all sorts of illegal things: speeding, smoking in cafés etc. Reflecting on this, we quickly realize that this 'infrastructure' would necessarily be so intrusive and inflexible that we would hardly be able to do anything useful, let alone have any fun.

In my opinion, one of the great security challenges ahead of us is what I call *audit-based compliance control*. Which is a way of doing compliance control, but by deterring rather than preventing infringements; that is, in an *a posteriori* fashion, as opposed to all present approaches, which work on an *a priori* basis. The principle is quite simple: rather than preventing illegitimate actions, we want to be able to detect them. So the responsibility of acting according to the agreed policies does not lie with the system (which cannot prevent all illegal actions anyhow), but rests with the user. What the system does is make a detailed log of its actions, so that if policies are not complied with, there is an effective way of finding out who has infringed them.

So in the presence of such a system, if Alice wants to share a new secret idea with Bob, who works at a different company, all she has to do is couple the document containing the idea with a policy saying that it is for Bob's eyes only, and send it to him. If Bob does not follow the policy, the logging system in place at Bob's premises will record it, and when the auditor visits Bob to check if he behaved correctly, he will be able to find the infringement. Clearly, Alice has no complete guarantee that Bob will actually follow the policy, but with the present systems she has no guarantee anyhow, and 100% security – as we have seen – is not something of this world.

The design and deployment of such a system is much more challenging than it may at first appear. There are three main problems:

1. Bridging the gap between the high-level policies and the low-level events that we can log. If Bob wants to send to Charlie the secret document he received from Alice, he can use a number of cryptographic tools to hide his actions from the logging systems.

2. Finding the one infringement in a log containing millions of entries is quite a bit more difficult than finding a needle in a haystack.
3. Privacy. Deep logging of everyone's actions is not quite privacy-friendly. People should be accountable for their wrong actions, but this does not entitle auditors to have a full record of everyone's private life.

These are three difficult problems that one day will be solved and will lead us to the realization of a completely new way of doing compliance control.
So far for the most challenging of my research dreams. I am confident that Eindhoven University of Technology, and 3TU.Federation, will be a wonderful environment in which to tackle it.

Education

The next thing I want to talk about briefly is education – which next to research is the other reason for the existence of universities and professors in the first place. There are some premises I want to make.

First, the Netherlands is a knowledge country. The Dutch government and the majority of us think and hope that the Dutch high-tech industry will be a winning factor in guaranteeing the maintenance of our level of economical prosperity. We are now a rich country; and we hope that technology will help us stay wealthy. To this end, the Dutch government is investing billions of euro in research and scientific innovation. As a scientist I am very pleased with this.

Secondly, I think we have good reasons to be happy about the quality of the Dutch universities.

So far the good news. Now the bad news:

First, despite good funding and good universities, Dutch college students are generally not attracted by a high-tech career. This can easily be demonstrated by looking at the number of students enrolling at technical faculties.

Second, Dutch students usually do not have the right preparation and attitude to succeed in a high-tech career. They are often not well-prepared when they arrive at university. It is clear that they are not accustomed to making big efforts for learning and mastering new concepts, particularly abstract ones.

Why is this happening? There are various reasons, many of which are beyond my own analytical abilities, and beyond the scope of this short dissertation. Nevertheless, I would like to point out a couple of them.

The Dutch school system

I am now going to talk about education in the Netherlands, but not at universities. I am going to focus on the range of schools between the elementary schools and the high schools.

From the viewpoint of the Dutch knowledge society, Dutch schools are a catastrophe.
Honestly, it took me a long time to understand why. Reality is in this case so far from my perception of how schools should be that it truly took me years before I became fully aware of the situation. And suddenly, one day, I realized something. Well, actually I read it in the newspaper, in one of the thousands of articles about Dutch education. This is the sentence that glued my feet to the ground:
"*In de informatiemaatschappij gaat het niet om kennis. Vaardigheden, dat is belangrijk*."
"In the information society, knowledge is not important, competences are."
This sad, ugly, and in my opinion wrong statement is directly translated by people who in my opinion are ruining generations of potential scientists in the motto of a large part of the Dutch school system.
"Knowledge is not important, competences are."
For example, it is not important to learn – say – *why* Pythagoras' theorem works. It is important to know how to use a calculator to compute the length of the hypotenuse.
The sad consequence of this viewpoint is that our kids learn less and less, do little or no homework, and when they eventually need to study something, like – say – the history of World War II, they do not really apprehend it, but are usually asked to write a *report* on it. So that our typical young student sits a few hours at the computer, copying and pasting from all sorts of sources on the internet, and re-editing it until he has created – it must be said – a very nice report.

The result is that the student learns to use his brain at meta-level: the knowledge on World War II went from one document to the other, through the computer, and never fully entered –let alone settled in – the brain of the student. What he learned is how to glue the pieces together, and how to wrap it up well, but the personal involvement in the heart of the matter is minimal. Students 'handle' and 'manage'

knowledge, rather than apprehending it, rather than making it theirs, rather than getting deep into the heart of the matter. Also, the scientific quality of the information they deal with is often very low, a fact that prevents them from developing a healthy critical sense with respect to the various sources.
Some schools are now abolishing books in favor of laptops. This is hideous.
We have to stop this.

Let me now open a short parenthesis: I have been very lucky to be allowed to go to Italy for a one-year sabbatical together with my whole family. So my children Max and Luca (at that time 6 and 8 years of age) went to the Italian school for one year, which is – to say the least – very classical in its approach: lots of facts, data, and homework. For the sake of truth, they did not like the homework part. Nevertheless, all of a sudden they started coming home from school with lots of stories to tell us, about prehistory, the Romans, biology, about all sorts of things. They enjoyed learning and were absolutely delighted to share this with us. Especially when they could teach their parents something they had forgotten. It was a joy to see how happy they were to learn new things. (By the way, here I am *not* saying that Italian schools are better than Dutch ones. This is not true in many respects, and is not the point anyhow.)

Coming back to Dutch schools, here we have intelligent children who love to learn, we have millions of potential young scientists around us, and what do we teach them at school? Skills, competences, *vaardigheden*. A true waste of talent.
As if what they wanted from us was to learn ‘competences’.
As if they enjoyed that.
As if – and this is perhaps more important from the sociopolitical viewpoint – having an army of teenagers who are very skilled at writing portfolios would help the Netherlands as a knowledge country. It does not. We do not need a country of report-writers, we need a country of scientists.
So, please, let us throw away all this nonsense. If we want to build the knowledge society there is *one* thing that our school has to teach our children:
Passion.
The passion for arts, for math, for gymnastics, for music, for the languages, for literature, for developing whatever talents children may possess. The school is there to give young men and women the tools to deploy their potential, and these tools are based on *knowledge*. Because it is hard to become a passionate musician if you don’t learn the notes first.
If we show kids how beautiful mathematics can be, rather than just teaching them how to use some counting tricks, we have the chance that when they have to go to

university they'll choose something beautiful like math, physics and computer science, rather than something else just because it gives them a good job.
In my case, I studied music and math, because I thought they were the most beautiful things I could learn. At the time I had to choose my study, I had no greater aspiration than developing and enjoying the arts I was good at (and sciences – particularly math - have a lot to do with art, because the reason why we like them is that they are *beautiful*).

So, what can we do? Well, to teach passion we need passionate teachers. But that is not a problem: schools are full of them. What we need to do is to allow them to *teach*. And to allow them to demand that students actually learn something. I want to stress this point once again: I strongly believe that Dutch teachers are good, passionate and well-prepared. It is the system that does not allow them to work well.
I am also not saying that schools need to be more difficult than they are now. Look for instance at American high schools. They are certainly not more challenging than Dutch ones, but they do whatever it takes to develop the talents of their students. Something that – here – we have completely forgotten.

This brings me to the second point I wanted to make about Dutch schools.
Allow me another parenthesis. This time about diversity. In the US, if a student is very good at something but he is at the same time a bit weird, then the school will tend to concentrate on his talent, and will help him at developing it. Chances are that teachers will put him forward as a bright example to be followed. In the US, being weird and brilliant is pretty cool.
At Dutch schools it is hard to be different. If you are weird and brilliant the school will put more effort into correcting the fact that you are weird (with psychologists, committee meetings and remedial teachers) than into stimulating you because you are brilliant. And the even sadder truth of the matter is that even if you are not weird but simply brilliant, showing this is often not appreciated. Not until you are – finally – at university. Chances are that – before then – the 'system' will tolerate you and that other students will isolate you. I have seen too many talented students who have had a very hard time throughout high school. They could finally be proud of their talent only when they reached university. Which is too late for many of them.
Too often I have reason to believe that one of the goals of Dutch schools is to make all students in a way 'equal' (within the given school system, MBO, HAVO, VWO...). It sounds honorable, but it is wrong. They should instead make an effort to make all students *different*, and happy to be so.

So please let us do our best to throw away the old adagio: “*doe maar normaal, want dan doe je al gek genoeg*”. Wij hebben heel veel gekken nodig om ons mooie kennisland in stand te houden!
Ladies and gentlemen, it is nice to know. Period.
But we need to teach this to our kids as early as we can.

Acknowledgments

This is for me the most important part of this speech, so please bear with me.

It is only right for me to start thanking my parents and family.
Cara mamma, caro papà. Avete sempre fatto tutto il possibile per assecondare e sviluppare le mie passioni e per sostenermi nei miei sogni. Avete sempre messo i miei interessi davanti ai vostri. Mi ritengo molto fortunato per questo, e senza il vostro costante supporto non sarei qui a parlarvi in questo momento. Vi ringrazio per questo di cuore. Silvana, tu sei sempre stata un'intelligentissima e importante confidente e alter ego. Le nostre chiacchierate hanno sempre portato chiarezza nei momenti di scelta.
Nicole, Max e Luca. Senza di voi non sarei qui, e anche se il lavoro ogni tanto mi ruba più ore di quanto noi tutti vorremmo, la vostra presenza e il vostro affetto sono il vero sestante della mia esistenza. Senza il vostro costante supporto e comprensione non avrei mai potuto dedicarmi alla carriera accademica. Vi sono immensamente grato del vostro sostegno, e del vostro amore. Grazie.
Coming back to academia, while being reasonably intelligent is a prerequisite for becoming a scientist, it takes more than that. There are very many people I should thank for turning me into a scientist; here I mention three of them hoping for the forgiveness of the others: my Italian professor Annalisa, my friend Maurizio, and in particular, Krzysztof Apt. Dear Krzysztof, with your brightness and scientific integrity, you have always been an epitome of the true scientist. Your example constantly helps me to discern good from bad science. Also, I am grateful to the CWI in Amsterdam for offering me an ideal place to develop my research interests during my PhD.
A few years after my PhD, at the University of Twente, I had two great fortunes: to find an outstanding boss and an outstanding research institute.
While being a decent scientist does not actually *prevent* you from becoming a full professor, it is certainly not enough. Pieter Hartel is the man who realized the miracle of turning the itinerant scientist I was seven years ago into someone who is now reasonably at ease with managing projects, with coaching co-workers, with starting new research directions and initiatives etc. Pieter, it is hard to put into words how much I owe you for this and for your friendship. And for fixing the mess I have been making every now and then. Every time I have a management or

leadership problem my first, second and third thoughts go to you and I try to imagine how you would handle it if you were in the same situation. Thanks.
I am also grateful to the CTIT – the research institute I participated in in Twente – and its directors Peter Apers and Iddo Bante. The CTIT contributed substantially to my development by giving me the lead of both the 'strategic research orientation' and the 'spearhead program' on security. These are internally funded projects which together exceed 2 million euro (I was assistant professor at the time). The money is meant to stimulate research in security by coordinating the efforts of various chairs working on different aspects of security. This was not only a unique opportunity for me, but I think it is also a wise manner to influence and characterize the research of a university.

The chair I now have the privilege of leading is a unique opportunity for which I want to thank the Eindhoven University of Technology and the CeDICT, the Centre for Dependable ICT Systems, one of the Centres of Excellence of 3TU. The Security chair participates in the security activity of the NIRICT, the Netherlands Institute for Research on ICT. I am grateful to Jos Baeten for fighting to have a Security chair at this university, and to the Executive Board for believing in me.
Last but by no means least, the people I work with and have worked with, and in particular the PhD students: Gabriele, Jordan, Ricardo, Marnix, Ari, Yee-Wei, Marcin, Ayse, Daniel, Bruno, Jing, Emmanuele and Damiano. You can't imagine how important your presence is to me. Without you all, I would have changed job long ago.

Ik heb gezegd.

References

1. Ross Anderson. *Security Engineering, Second Edition*. Wiley.

Curriculum Vitae

Prof.dr. Sandro Etalle was appointed full-time professor of Embedded System Security in the Department of Mathematics and Computer Science of Eindhoven University of Technology (TU/e) on 1 October 2007.

Sandro Etalle (1965) graduated *cum laude* in Mathematics at the University of Padova in 1991. He carried out his PhD research partly at the University of Padova under the supervision of prof. Annalisa Bossi and mostly at the CWI (National Research Institute for Mathematics and Computer Science) under the supervision of prof.dr. Krzysztof Apt. In 1995 he gained his PhD in Computer Science from the University of Amsterdam. He worked for the Universities of Amsterdam, Genova and Maastricht before joining the University of Twente in 2001. After a period visiting the University of Trento, he now leads the Security group at the TU/e, and works for the University of Twente one day a week. Sandro Etalle started researching the verification of security protocols in 2001. Since then, his main research focus has been policy enforcement and the protection of confidential data. Currently, his interests include intrusion detection and risk management.

Colophon

Production
Communicatie Expertise
Centrum TU/e
Communicatiebureau
Corine Legdeur

Cover photography
Rob Stork, Eindhoven

Design
Grefo Prepress,
Sint-Oedenrode

Print
Drukkerij van
Santvoort, Eindhoven

ISBN ???
NUR ???

Digital version:
www.tue.nl/bib/